Amendments to the Specification

Please replace the paragraph on page 1, lines 2 to 3 with the following amended paragraph:

This application is a continuation-in-part application of United States Patent Application No. [[98]] 08/426,090.

Please replace the paragraph on page 4, lines 11 to 13 with the following amended paragraph:

i) a first of said correspondents A selecting a first random integer x and exponentiating a function $f(\alpha)$ including said generator to a power $[[g^{(x)}]]$ g(x) to provide a first exponentiated function $f(\alpha)^{g(x)}$;

Please replace the paragraph on page 4, lines 16 to 18 with the following amended paragraph:

iii) said correspondent B selecting a second random integer y and exponentiating a function $f(\alpha)$ including said generator to a power $[[g^{(y)}]]$ g(y) to provide a second exponentiated function $f(\alpha)^{g(y)}$;

Please replace the paragraph on page 4, lines 19 to 23 with the following amended paragraph:

iv) said second correspondent B constructing a session key K from information made public by said first correspondent A and information that is private to said second correspondent B, said session key also being constructible by said first correspondent A ~~for~~ from information made public by B and information that is private to said first correspondent A;

Please replace the paragraph on page 4, lines 28 to 30 with the following amended paragraph:

vi) said second ~~of said correspondents~~ correspondent B forwarding a message to said first correspondent A including said second exponential function $f(\alpha)^{g(y)}$ and said value h of said cryptographic function F[ð,K];